UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,121	08/15/2001	Toyoaki Kishimoto	212668US6	1335

22850 7590 05/06/2010

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
05/06/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	09/929,121	KISHIMOTO, TOYOAKI	
	Examiner	Art Unit	
	Tamara Teslovich	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,7,9,11 and 13-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,7,9,11 and 13-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to Applicant's remarks and amendments filed December 3, 2009.

Claims 1, 3-5, 7, 9, 11, and 13-18 are pending and herein considered.

Response to Arguments

Applicant's arguments filed December 3, 2009 have been fully considered but they are not persuasive.

The Examiner respectfully disagrees with Applicant's arguments concerning Cooper's alleged failure to teach or suggest "generating, at a Web browser of the mobile information terminal, a secret key based on a result of the verification" and "encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server." Applicant's remarks are based on the assertion that the generation of any key, be it secret or public, is done outside the mobile device and as such, Cooper fails to anticipate Applicant's claims. The Examiner would like to draw attention to portions of the Cooper reference, including but not limited to paragraphs 34, 38, 50-51, 137,165, 232, 281-282, 284 and 289-290 wherein Cooper discloses the use of web browsers within mobile information terminals (par 38) whereby any and all necessary keys, digital certificates, and watermarks may be generated. Cooper describes in these portions how clients may use API and java applets running on their workstations to generate signed keys for existing certificates (pars 282-282 and 284). He also discloses that it is "contemplated by this application that each user device

115 will have some way to both store and manage digital certificates" (par 165) and how it is not unusual for any given user device 115 to have numerous digital certificates as it logs on to new website and performs other Web or Internet operations (par 164). He also discusses how "virtually all Web Browser programs, including for example Netscape and Internet Explorer, have mechanisms to store and manipulate encryption keys and digital certificates" and that it "is common to see an area reserved for the creation, storage, and usage of digital certificates under the menu item named 'options' or 'preferences' in such Web Browser programs" (par 137). Cooper goes on in paragraphs 281-282 to describe how customers may easily modify their existing software to call the certificate and watermarking functions provided by a customer distribution system and how a Java applet running on a client workstation may operate outside the Java sandbox, giving it access to low level Windows and Unix functions allowing it to accept requests necessary to install and retrieve certificates. In paragraph 284, Cooper even teaches how the supplied software installed at the customer site may be used to generate a signed key for an existing certificate. In paragraphs 289-290 Cooper further discloses how a customer may easily modify their existing software to call the content distribution system certificate and watermarking modules including API calls for creating, installing, and retrieving digital certificates between the CA server and a client workstation. It is based upon these portions in view of the reference in its entirety that the Examiner maintains her position that Cooper anticipates generating, at a Web browser of a mobile information terminal, a secret key based on a result of the

verification of a certificate authority and encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server.

It is based on the arguments presented above in view of the references in their entirety that the Examiner maintains her rejection of the claims, presented below for Applicant's convenience.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-5, 7, 9, 11 and 13-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 6,248,946 to Norman Dwek and further in view of US Patent Application Publication 2001/0051996 A1 to Cooper et al.

Regarding ***Claim 1***, Dwek teaches a user authentication method for an authentication server which executes user authentication between an information terminal and a content providing server interconnected by an open network, comprising the steps of:

registering, at an authentication server, unique identification information (col.4 lines 31-43);

presenting, from the authentication server, to said mobile information terminal, a recommended menu including a plurality of official site access information for accessing predetermined content providing servers, respectively (col.4 lines 26-30 and 43-67; col.10 lines 4-24);

receiving, at the authentication server, from said information terminal, the unique identification information, and a request for registering one of said official site access information for accessing said content providing server with a personal menu via the open network (col.9 lines 31-45; col.10 lines 21-47 and 60-67);

determining, at the authentication server, whether said unique identification information received from said information terminal is registered with said customer database (col.12 lines 15-21; col.15 lines 34-40);

sending a notification from the authentication server to said content providing server by which said requested site is produced, that starting of service provision for said information terminal be permitted, if the unique identification information is found registered with said customer database (col.12 lines 15-21; col.15 lines 34-40);

registering, at the authentication server, said requested official site access information with said personal menu after receiving an acknowledgement response of said notification from said content providing server (col.10 lines 13-67); and

notifying, to said information terminal from said authentication server, a completion of said registration (col.10 lines 35-51).

Dwek fails to teach the abovementioned system wherein the information terminal is a "mobile information terminal" and wherein the unique information corresponds to a mobile information terminal and includes a manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal and wherein that information is encrypted by a secret key at the Web browser installed on said mobile information terminal.

Dwek also fails to specifically teach transmitting, from said mobile information terminal to said authentication server, a request to connect to the authentication server, transmitting, from said authentication server to said mobile information terminal, a certificate including a public key of the authentication server, an expiration date of the certificate and a digital signature, verifying an identity of the authentication server at the mobile information terminal based on the received certificate, generating, at a Web browser of the mobile information terminal, a secret key based on the result of the verification, encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server and transmitting the encrypted secret key from the mobile information terminal to the authentication server.

Cooper teaches a network based content distribution system including a plurality of mobile information terminals (pars 31, 33, 38) wherein each of the devices includes a unique manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal (pars 159-

161) and wherein that information is transmitted in an encrypted form by a secret key (pars 39, 43, 52, 58 "encrypted") at the web browser (pars 35, 38, 50, 51, 137, 149 "browser") installed on the mobile information terminal (pars 283, 291 "SSL").

Cooper also teaches transmitting, from said mobile information terminal to said authentication server, a request to connect to the authentication server (pars 140-145; 273-277), transmitting, from said authentication server to said mobile information terminal, a certificate including a public key of the authentication server, an expiration date of the certificate and a digital signature (pars 145-148, 277), verifying an identity of the authentication server at the mobile information terminal based on the received certificate (par 165), generating, at a Web browser of the mobile information terminal, a secret key based on the result of the verification (pars 197-198, 227, 277), encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server (par 225, 277), and transmitting the encrypted secret key from the mobile information terminal to the authentication server (par 218, 227);

It would have been obvious to a person of average skill in the area at the time of the invention to include within Dwek the wireless and security capabilities as described in Cooper as well as the request, certificate, secret key and public key disclosed by Cooper in order to provide for users connected to the Internet and other media and document servers via mobile information terminals such as cellular phones and other handheld devices in a secure and reliable manner.

Regarding ***Claim 3***, the combined method of Dwek and Cooper teaches the user authentication method according to Claim 1, wherein, when registering said site access information, user authentication is performed on the basis of said unique identification information and said mobile information terminal requested to make display for prompting said user to enter a password of the user (Cooper par 126, 148-149, 205, 218).

Regarding ***Claim 4***, the combined method of Dwek and Cooper teaches the user authentication method according to Claim 3, wherein, in the registering, a charging server is instructed to charge said user for the use of a service provided by said content providing server associated with said site access information at the time of registering said site access information (Dwek col.12 lines 15-21; col.15 lines 35-40).

Regarding ***Claim 5***, the combined method of Dwek and Cooper teaches the user authentication method according to Claim 4, wherein, in the registering, confirming, before instructing said charging server for the charging, that said user is a registered user of said charging server is included (Dwek col.12 lines 15-21; col.15 lines 35-40).

Regarding ***Claim 7***, the combined method of Dwek and Cooper teaches the user authentication method according to Claim 1, wherein the unique identification information is read, by said Web browser, from a flash memory (Cooper pars 39, 126,

130) installed on said mobile information terminal and the retrieved unique identification information is transmitted as encrypted (Cooper pars 39, 43, 52, 58 "encrypted") by the predetermined encryption algorithm by said Web browser (Cooper pars 35, 38, 50, 51, 137, 149 "browser") (Dwek col.5 lines 31-43).

Regarding ***Claim 9***, Dwek teaches a user authentication server which executes user authentication between a information terminal and a content providing server interconnected by an open network, comprising

means for registering unique identification information corresponding to said information terminal (col.4 lines 31-43);

means for presenting, to said information terminal, a recommended menu including a plurality of official site access information for accessing predetermined content providing servers, respectively (col.4 lines 26-30 and 43-67; col.10 lines 4-24);

means for receiving, from said information terminal, the unique identification information and a request for registering one of said official site access information for accessing said content providing server with a personal menu via the open network (col.9 lines 31-45; col.10 lines 21-47 and 60-67);

means for determining whether the unique identification information received from said information terminal is registered with said customer database (col.12 lines 15-21; col.15 lines 34-40);

means for sending a notification to said content providing server, by which said requested site is produced, that starting of service provision for said information terminal be permitted, if the unique identification information is found registered with said customer database (col.12 lines 15-21; col.15 lines 34-40);

means for registering the requested official site access information with said personal menu after receiving an acknowledgement response of said notification from said content providing server (col.10 lines 13-67); and

means for presenting, to said information terminal, a completion of said registration (col.10 lines 35-51).

Dwek fails to teach the abovementioned system wherein the information terminal is a “mobile information terminal” and wherein the unique information corresponds to a mobile information terminal and includes a manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal and wherein that information is encrypted by said secret key at the Web browser installed on said mobile information terminal.

Dwek also fails to specifically teach means for receiving a request to connect from the mobile information terminal, means for transmitting a certificate to the mobile information terminal, the certificate including a public key of the user authentication server, an expiration date of the certificate and a digital signature, and means for receiving a secret key from the mobile information terminal that is encrypted using the public key of the user authentication terminal, the secret key being generated by a Web

browser at mobile information terminal after verifying an identity of the authentication server at the mobile information terminal based on the received certificate.

Cooper teaches a network based content distribution system including a plurality of mobile information terminals (pars 31, 33, 38) wherein each of the devices includes a unique manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal (pars 159-161) and wherein that information is transmitted in an encrypted form by a secret key (pars 39, 43, 52, 58 "encrypted") by a web browser (pars 35, 38, 50, 51, 137, 149 "browser") installed on the mobile information terminal (pars 283, 291 "SSL") .

Cooper also teaches means for receiving a request to connect from the mobile information terminal (pars 140-145; 273-277), means for transmitting a certificate to the mobile information terminal, the certificate including a public key of the user authentication server, an expiration date of the certificate and a digital signature (pars 145-148, 277), and means for receiving a secret key from the mobile information terminal that is encrypted using the public key of the user authentication terminal, the secret key being generated by a Web browser at mobile information terminal after verifying an identity of the authentication server at the mobile information terminal based on the received certificate (pars 197-198, 218, 225, 227, 277).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Dwek the wireless and security capabilities as described in Cooper as well as the request, certificate, secret key and public key disclosed by Cooper in order to provide for users connected to the Internet and other media and

document servers via mobile information terminals such as cellular phones and other handheld devices in a secure and reliable manner.

Regarding ***Claim 11***, the combined method of Dwek and Cooper teaches the user authentication server according to claim 9 wherein the unique identification information is read, by said Web browser, from a flash memory (Cooper pars 39, 126, 130) installed on said mobile information terminal and the retrieved unique identification information is transmitted as encrypted (Cooper pars 39, 43, 52, 58 "encrypted") by the predetermined encryption algorithm by said Web browser (Cooper pars 35, 38, 50, 51, 137, 149 "browser") (Dwek col.5 lines 31-43).

Regarding ***Claim 13***, Dwek teaches a user authentication server which executes user authentication between a information terminal and a content providing server interconnected by an open network, comprising:

a registering module configured to register unique identification information corresponding to said information terminal received from the information terminal with a customer database of said authentication server (col.4 lines 31-43);

an interface configured to present, to said information terminal, a recommended menu including a plurality of official site access information for accessing predetermined content providing servers, respectively (col.4 lines 26-30 and 43-67; col.10 lines 4-24);

an interface configured to receive, from said information terminal, the unique identification information and a request for registering one of said official site access

information for accessing said content providing server with a personal menu via the open network (col.9 lines 31-45; col.10 lines 21-47 and 60-67);

a determination module configured to determine whether the unique identification information received from said information terminal is registered with said customer database (col.12 lines 15-21; col.15 lines 34-40);

an interface configured to transmit a notification to said content providing server, by which said requested site is produced, that starting of a service provision for said information terminal be permitted, if the unique information is found registered with said customer database by the determination module (col.12 lines 15-21; col.15 lines 34-40);

a registering module configured to register the requested official site access information with said personal menu after receiving an acknowledgement response of said notification from said content providing server (col.10 lines 13-67); and

an interface configured to present, to said information terminal, a completion of said registration (col.10 lines 35-51).

Dwek fails to teach the abovementioned system wherein the information terminal is a “mobile information terminal” and wherein the unique information corresponds to a mobile information terminal and includes a manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal and wherein that information is encrypted by a predetermined encryption algorithm by a Web browser installed on said mobile information terminal.

Dwek also fails to specifically teach an interface configured to receive a request to connect to the user authentication server from the mobile information terminal, an interface configured to transmit a certificate including a public key of the user authentication server, an expiration date of the certificate and a digital signature to said mobile information terminal, and an interface configured to receive a secret key from the mobile information terminal that is encrypted using the public key of the user authentication terminal, the secret key being generated by a Web browser at mobile information terminal after verifying an identity of the authentication server at the mobile information terminal based on the received certificate.

Cooper teaches a network based content distribution system including a plurality of mobile information terminals (pars 31, 33, 38) wherein each of the devices includes a unique manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal (pars 159-161) and wherein that information is transmitted in an encrypted form by a predetermined encryption algorithm (pars 39, 43, 52, 58 “encrypted”) by a web browser (pars 35, 38, 50, 51, 137, 149 “browser”) installed on the mobile information terminal (pars 283, 291 “SSL”) .

Cooper also teaches an interface configured to receive a request to connect to the user authentication server from the mobile information terminal (pars 140-145; 273-277), an interface configured to transmit a certificate including a public key of the user authentication server, an expiration date of the certificate and a digital signature to said mobile information terminal (pars 145-148, 277), and an interface configured to receive

a secret key from the mobile information terminal that is encrypted using the public key of the user authentication terminal, the secret key being generated by a Web browser at mobile information terminal after verifying an identity of the authentication server at the mobile information terminal based on the received certificate (pars 197-198, 218, 225, 227, 277).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Dwek the wireless and security capabilities as described in Cooper as well as the request, certificate, secret key and public key disclosed by Cooper in order to provide for users connected to the Internet and other media and document servers via mobile information terminals such as cellular phones and other handheld devices in a secure and reliable manner.

Regarding **claim 14**, the the combined method of Dwek and Cooper teaches the authentication server according to Claim 13, wherein the recommended menu including a plurality of official site access information includes a plurality of hierarchical levels of categories (Dwek col.10 lines 4-20).

Regarding **claim 15,** the combined method of Dwek and Cooper teaches the authentication server according to Claim 13, wherein the customer database is configured to store a name, age, birthday, gender and address corresponding to a user (Dwek col.10 lines 4-20, 52-59).

Regarding **claim 16**, the combined method of Dwek and Cooper teaches the authentication server according to Claim 15, wherein the authentication server uses at least one of the name, age, birthday, gender and address corresponding to a user to generate the recommended menu (Dwek col.10 lines 4-20, 52-59).

Regarding **claim 17**, the combined method of Dwek and Cooper teaches the authentication server according to claim 13, wherein the personal menu includes a plurality of icons, each of which corresponds to a link to a website external to the authentication server (Dwek col.9 lines 58-66; col.10 lines 35-47).

Regarding **claim 18**, the combined method of Dwek and Cooper teaches the authentication server according to claim 13, wherein the authentication server and the content providing server are remotely connected via the Internet (Dwek col.4 lines 53-67).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437